

WHEN DOES A "HACKER" BECOME AN "ATTACKER?"

**A MONOGRAPH
BY
Major David C. Are
Signal Corps**

**School of Advanced Military Studies
United States Army Command and General Staff
College
Fort Leavenworth, Kansas**

First Term AY 98-99

Approved for Public Release Distribution is Unlimited

DNC QUALITY INSPECTED

19990804 036

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE
17 December 1998

3. REPORT TYPE AND DATES COVERED
Monograph

4. TITLE AND SUBTITLE

When does a "Hacker" become an "Attacker?"

5. FUNDING NUMBERS

6. AUTHOR(S)

MAJOR DAVID C. ARE

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

School of Advanced Military Studies
Command and General Staff College
Fort Leavenworth, Kansas 66027

8. PERFORMING ORGANIZATION
REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Command and General Staff College
Fort Leavenworth, Kansas 66027

10. SPONSORING / MONITORING
AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE
DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)
SEE ATTACHED

14. SUBJECT TERMS

Hacker
Cyberwar

15. NUMBER OF PAGES

61

16. PRICE CODE

17. SECURITY CLASSIFICATION
OF REPORT
UNCLASSIFIED

18. SECURITY CLASSIFICATION OF THIS
PAGE
UNCLASSIFIED

19. SECURITY CLASSIFICATION
OF ABSTRACT
UNCLASSIFIED

20. LIMITATION OF ABSTRACT
UNLIMITED

ABSTRACT

WHEN DOES A "HACKER" BECOME AN "ATTACKER?" By MAJ David C. Are, USA, 59 pages.

The ability to defend the United States cyber sovereign territory is a must for the country to continue to enjoy relative freedom. The actual defense of this is far more difficult than the traditional defense of land, sea or air space. The Internet offers an environment of exponential growth in both technology and users. Couple this with an infantile and developing governing system and the Internet is both a conduit for use and a vehicle for attack.

The history of cyber attack is key in determining the ability to defend and the mode in which to do it. By tracing the capabilities of adversaries, both internal and external, we can attempt to delineate the point where the electronic intrusion becomes alarming to the nation. Combine this understanding with a thorough knowledge of current methodologies and tools used for cyber attack and one has a good jump on "knowing one's enemy."

Constraining, yet legitimizing, the effort of governments to fight the unbounded attack of cyber warriors are laws and agreements which attempt to lay ground rules for cyber utilization. Careful construction of these rules joined with vigilant international agreements can facilitate apprehension and thwarting of would-be attackers worldwide. Laws which are drafted without thought to the defense of information systems can be equally as damaging to the government that adopts them.

This monograph concludes with the current efforts underway by the United States government and the Department of Defense in particular. Presidential Decision Directives 62 and 63 posture the United States for success in combating cyber aggression. The follow through by the legislative, judiciary branches and various departments will determine the success of this country in securing its national information infrastructure.

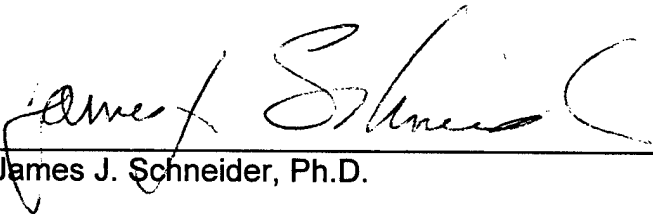
SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

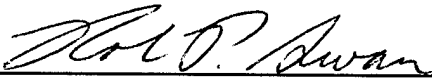
Major David C. Are

Title of Monograph: *When Does the A "Hacker" Become An "Attacker?"*

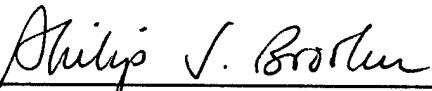
Approved by:


James J. Schneider, Ph.D.

Monograph Director


LTC Robin P. Swan, MMAS

Director, School of Advanced
Military Studies


Philip J. Brookes, Ph.D.

Director, Graduate Degree
Program

Accepted this 16th Day of December 1998

ABSTRACT

WHEN DOES A "HACKER" BECOME AN "ATTACKER?" By MAJ David C. Are, USA, 59 pages.

The ability to defend the United States cyber sovereign territory is a must for the country to continue to enjoy relative freedom. The actual defense of this is far more difficult than the traditional defense of land, sea or air space. The Internet offers an environment of exponential growth in both technology and users. Couple this with an infantile and developing governing system and the Internet is both a conduit for use and a vehicle for attack.

The history of cyber attack is key in determining the ability to defend and the mode in which to do it. By tracing the capabilities of adversaries, both internal and external, we can attempt to delineate the point where the electronic intrusion becomes alarming to the nation. Combine this understanding with a thorough knowledge of current methodologies and tools used for cyber attack and one has a good jump on "knowing one's enemy."

Constraining, yet legitimizing, the effort of governments to fight the unbounded attack of cyber warriors are laws and agreements which attempt to lay ground rules for cyber utilization. Careful construction of these rules joined with vigilant international agreements can facilitate apprehension and thwarting of would-be attackers worldwide. Laws which are drafted without thought to the defense of information systems can be equally as damaging to the government that adopts them.

This monograph concludes with the current efforts underway by the United States government and the Department of Defense in particular. Presidential Decision Directives 62 and 63 posture the United States for success in combating cyber aggression. The follow through by the legislative, judiciary branches and various departments will determine the success of this country in securing its national information infrastructure.

TABLE OF CONTENTS

I. CHAPTER 1

Introduction.	1
Background	2
What is the Internet and what does it mean to the United States?	3
What defines the domain where cyber and hacker warfare exists?	6

II. CHAPTER 2

What constitutes an attack?	9
---------------------------------------	---

III. CHAPTER 3

Historical background for cyber attack	13
Historical foundation for use of information warfare	15
What are some targets?.	16
What are the tools used for attack/defense?	17
What are some defensive measures?	21
What are the trends in attack?.	23

III. CHAPTER 4

Legalities	25
What are the International laws concerning cyber use?	25
What are the United States laws concerning cyber use?	28
What are some historical precedents of convictions (International and US)?	29

IV. CHAPTER 5

Computer Network Defense Joint Task Force (CND JTF)	34
What is the mission and does it support the NSS and NMS?	34
What is the projected unit environment for the CND JTF?	37

V. CHAPTER 6

Current defensive efforts and trends	39
Defensive measures being taken	40

VI. CHAPTER 6

Conclusion 43

Endnotes 45

Bibliography. 48

CHAPTER 1

Introduction-

Attack, and subsequent defense of a nation state's sovereign territory, constitutes warfare. The necessity to defend borders to ensure national survival is as old as the nation state itself. The early twentieth century saw the first expansion of this territorial defensible terrain where air power turned the relative two-dimensional battlefield into a three-dimensional one. As the twentieth century draws to a close and the next millennium approaches, we see the rapid and widespread incorporation of another dimension into the "territory" of nations. Cyberspace presents, to date, limitless space for countries to offer citizens the ability to connect many aspects of their lives from the relative comfort of their home or office. As the utilization of this web proliferates, so does the vulnerability of the players that use this "space." The struggle for this space and the manipulation and control of it is considered information warfare.

Defense of cyber borders takes a different form than the traditional defense of geographical borders. With no forward line of troops and no discernibly defensible terrain boundaries, the cyber realm is much harder to defend. To further complicate the matter these entry points are not discrete points which are easily observable. In the realm of information warfare, pertinent questions become what constitutes the nature of attack and defense? Do the national laws of the United States as well as the international laws and agreements facilitate the current efforts which support the National Security Strategy (NSS) and the National Military Strategy (NMS)?

This monograph details the current environment for the conduct of cyber warfare. Within this environment, a basic foundation is set to ensure an understanding of historical

footing, current laws and legal trends. Trends of attack and defense are also discussed. From these a profile of the modern-day computer-attacker is derived. Once the profile of the attacker is established the tools for attack are defined. This tool set along with the bounded attack profile allow computer defense organizations to develop and field viable defense forces. The United States approach to this defense is presented using initiative and defense strategies currently being established. The Computer Emergency Response Team (CERT) and the Department of Defense (DOD) Computer Network Defense Joint Task Force (CND-JTF) are the fighters which will defend the United States against cyber attacks now and in the near future.

Background

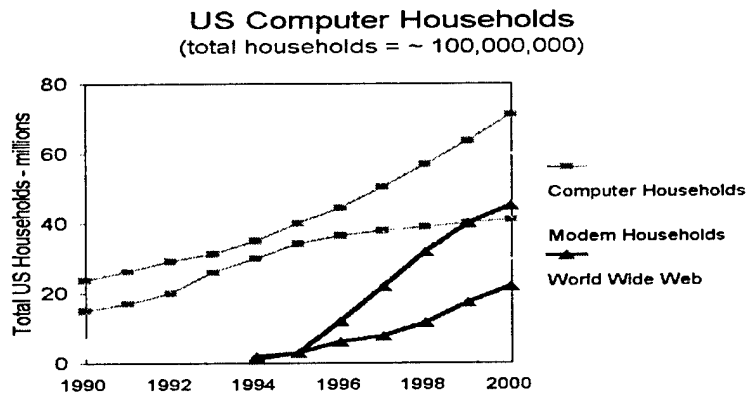
The spectrum of conflict is as old as human interaction itself. The human ability to influence other humans through armed conflict has been a constant throughout history. Accepted theorists have proposed a multitude of causes of war and history. What these two sources suggest is the actual makeup of warfare: the real battles, the actual winners and losers. These, in contrast to the makeup of the enabling factors and the outcomes, are actually constant in their composition. The main ingredients for the recipe for battle simply consist of attack and defense. Other aspects support this, such as deception, logistics and intelligence, but the battle is simply interactions of attack and defense. "[T]he subjugation of the enemy is the end, and the destruction of his fighting force the means" says Clausewitz.¹ This is certainly as true in the physical warfare world today as it was in the days of Thucydides and ancient Greece. The ability to subjugate, or be subjugated, depends on the will of the people, abilities of the leader, and the capabilities

of the armies of that nation. The power, whether relative or perceived is as vital to nation state survivability as ever in history. But does this apply today in the world where we have electronic avenues throughout every aspect of civilization? The simple truth appears to be yes.

As we see the ability to wage conflict spread into the electronic arena, we see the range of those who can initiate conflict spread as well. The Maoist theory of war lends itself to the efforts of the population and the need of the citizen to join in the warfighting effort.² The fact that the lust for power extends to the information arena is just a continued progression in the dimensional world. Anne Wells Branscomb states, "[I]n virtually all societies, control of and access to information became instruments of power, so much so that information came to be bought, sold and bartered by those who recognized its value."³ This also incorporates the vulnerabilities of the infrastructure of a nation state to these same belligerent efforts.

What is the Internet and what does it mean to the United States?

The Internet represents the most encompassing interconnection of life ever introduced to man. The roots of the Internet are with the United States Department of Defense Information Processing Techniques Office (IPTO) and the Advanced Research Projects Agency (ARPA). In 1967, an effort was undertaken initially to ensure national level command and control communications were capable in a nuclear exchange. This quickly transitioned into an initiative to interconnect computing assets, both electronic and human, of academic and governmental agencies. The DOD continued to host this due to its ability fiscally to support this undertaking.



Rivalled only by the combined spread of telephony (both wired and cellular)⁴ computer use touches most lives and certainly affects all. With over 11,000,000 home personal computers linking into over 2,000,000 networks or subnetworks this mesh is unparalleled in its power as well as its complexity. "Like Einstein's universe, most networks are finite but unbounded. There's only a certain number of computers attached, yet you never quite reach the edge of the network. There's always another computer down the line."⁵ Each of these networks interconnect to each other, so it is easy to see the exponential spread of this technological enabler. The power⁶ of each of these separate entities is governed only by the drive of the human or organization which uses the system and the financial backing to maintain the necessary, virtually continual upgrades. "The computer has become a common denominator that knows no intellectual, political, or bureaucratic bounds: the Sherwin Williams of necessity that covers the world, spanning all points of view."⁷ As the computer becomes as commonplace as the light bulb, it will also become as irreplaceable as the light bulb which sheds light on the necessity and vulnerability of the technology itself.

In an attempt to wrap our arms around the different subsets of capabilities that the Internet offers the people of the United States, the DOD has collected the services into the National

Information

Infrastructure (NII)

and a subset called

the Defense

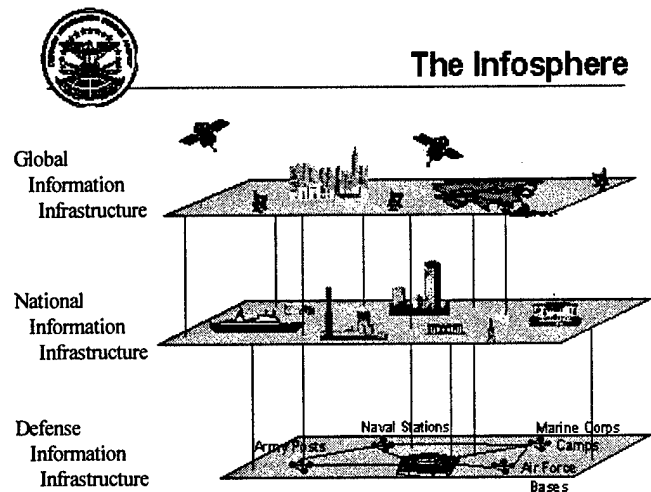
Information

Infrastructure

(DII).⁸⁹

The

interdependence of these two systems is indistinguishable and the reliance on one another is equally unmatched. "Their seamless relationship makes the distinguishing between them impossible"¹⁰ Any attack or intrusion on one can be construed as an attack on the other. Likewise any damage to one can equally damage the other and will definitely degrade the production capabilities of the other.



What defines the domain where cyber, hacker, and infrastructure warfare exist?

The overall domain for the conduct of information warfare is both broad (too broad) and vaguely defined given the scope and infancy of the method. This is clearly evident by Thomas Rona's early definition: "[T]he strategic, operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives."¹¹ This definition encompasses all aspects of information warfare, but fails to give definition to the boundaries for in-depth study.

For cyber, and hacker war the environment is clearly the electronic networks facilitating the information flow of governments, ministries, corporations, organizations and individuals as well as the interconnection of these networks. "No area of criminal activity has greater international implications than high technology crime because of the global nature of information networks. Computer hackers and other cyber-criminals are not hampered by international boundaries, since information can be transmitted quickly and covertly via telephone and information systems."¹² Just as the sky is the medium for airline traffic and aerial combat alike, so is the Internet the medium for electronic traffic and electronic combat. Infrastructure warfare can exist over several means including physical destruction. For purposes of this paper, we will address only the manipulation of infrastructure systems via electronic alteration of information systems that control these national backbone support facilities and systems.

Within the context of this network of interconnected and mutually supporting actors, the information systems, and the information that resides in it have increasing importance to warfare and national security. The act of war is "imposing the enemy to ones will."¹³ To that end, the control of information can and will not only support the physically destructive war efforts of the future, but could take a lead roll in the act of war itself.

The domain of conflict for the future of war exists not only within the confines of a nation's borders but can and will transcend international borders via communications links and infrastructure interconnectivity. The aspect of national sovereignty, as of yet, does not apply to electronic territorial position. This further complicates the attempt to grapple with the battlespace of IW. "(T)he ability of signals to travel across international networks and affect systems in distant countries conflicts with the long-standing principle of national, territorial sovereignty."¹⁴ The attacker can, and most likely will, enjoy the confines and relative security of residing in his host country.

In sum, the conflict domain is easy to define simply as the Internet. The simplicity of the denotation of the battlespace ends with this very broad ascertainment. The originator, sponsorship, detection, target, effect, and intention of the attack are much harder to define. Within the confines of United States moral ethics and infant (or non existent) international laws, the precise definition of the exact space is ambiguous at best. From the detection of a cyber intruder to the prosecution of cyber warfare, intent is often hard to determine and equally as undetectable.

As we survey the field of battle used for the conduct of cyber war, we may attempt to visualize how this war will be conducted. From the internal attacks from

discontented or disgruntled citizens to the attempted takedown of a foreign power, the weapons and levels of attack may vary. These levels of attack do not correspond to the effects that can be caused however. When do we know we are under attack and what can we do about it? this question will be addressed in the next chapter.

CHAPTER 2

What constitutes an attack?

Within the cyber world, attack is not dissimilar to the attack in the physical world. The current worldwide viewpoint of a cyber “attack” stems from research done at the Carnegie Mellon Software Engineering Institute. This think-tank later grew into the first Computer Emergency Response Team (CERT) Coordination Center in the United States. This CERT team serves as the blueprint for most cyber defense organizations already in existence. The definitions developed from this research serve as the current baseline for the promulgation of computer defense.

An attack is “a single unauthorized access attempt, or unauthorized use attempt, regardless of success.”¹⁵ This accepted definition not only gives a starting basis for dialogue, but expressed two very strong points. The first point is that the attack must only be a singular unauthorized access. The second is that the level of success of the attacker does not factor into the equation. Both of these qualifiers factor into the structure and mission of any defense force when dealing with computer defense.

A danger in utilizing this definition is the possibility of over extension of assets for the defense. Using the above mentioned definition, a seven-year-old child learning computers in her second grade class who happens to mistype a destination address is equally as guilty of attack as the foreign subversive who intends to end the current governments reign. To identify, investigate and respond to the possible attack scenarios could be both unrewarding and definitely over burdensome.

To help grapple with the above mentioned problem, Carnegie Mellon’s Dr. Howard developed two more definitions which help classify attacks. The first is the

“incident” and the second is the “incident classification.” An “incident involves a group of attacks that can be distinguished from other incidents because of the distinctiveness of the attackers, and the degree of similarity of sites, techniques, and timing.”¹⁶ The incident classification “indicates something about the type or quality of an incident.” It also “is some measure of quantity or severity that distinguishes incidents from one another, and when accumulated, gives an indication of overall Internet security.”¹⁷

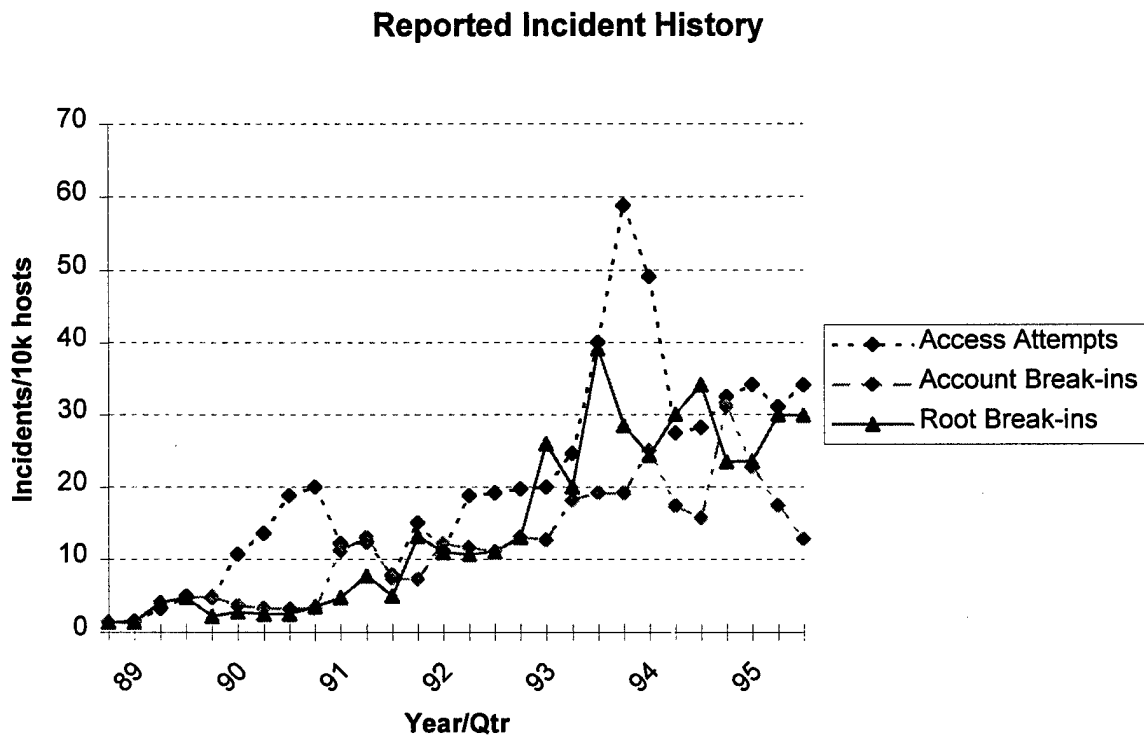
Within, and supported by, the definition of incident lies three distinct classifications. The least damaging level is the “access attempt.” This is when an attacker simply attempts to access a system. It is seen as an unsuccessful attack but counted as an attack just the same. The second grader fits into this category. This level of attack is nominally logged, counted and used for statistical data only.

The next and intermediate level is known as an “account break-in.” In the account break-in, an authorized user’s account is compromised and accessed. This can occur via multiple means including password bypass, theft and backdoor entry. This attack can cause as much damage as the account has access. This is a very effective method for theft and exploitation of sensitive material.

The third, and most potent of attacks, is the “root break-in.” In the root break-in, the actual control of the information system is violated. From the root, all accounts can be accessed and more importantly the functioning of the system itself can be manipulated. Any event from a total download of all information to system slowdown or crash can be accomplished from the root.

The second and third level incidents pose the greatest potential threat for any information system user including the US DOD. As the number of systems within the

Internet increase, the number of potential attackers increases. The chart below shows the growth of host attacks as reported. Although the first level incidents can be skewed due to education of users, second graders etc, the level two and three incidents clearly show the potential damage for systems¹⁸.



Key to note is that the chart only represents the reported cases. In 1995 a DOD exercise was conducted on the level of computer defense DOD-wide. Of the 8932 attempts to access root directories, an 88% success rate was reported. Of these successes, only 320 were reported (3.6% detected). Of these, only 22 were reported (.25% reported).¹⁹ Given this type of reporting record, the number of actual incidents could actually be in the millions per year.

Cyber attacks occur. The rising number of attacks is linked not only to the rising number of Internet connections and users, but also to the ever increasing intelligence of

the users on it. The effortless transferal of weapons to be used in attacks offers the attacker the ability to “shoot”, “scoot” and “hide” in and amongst the electronic trees of the Internet itself. The ability to detect incidents, report them and disseminate their effects is a major contributor to a successful defense. This will not be a deterrent in itself. The trends of attack show the constant upgrade of attack. Chapter 3 examines the nature of these historical trends.

CHAPTER 3

Historical background for cyber attack -

The genesis of cyber attack occurred and is reported in great detail in a book entitled The Cuckoo's Egg by Dr. Clifford Stoll. Dr. Stoll is a computer specialist within the astronomy field. His current occupation, as of the time of the book, is a computer product specialist for the Lawrence Livermore Labs in Berkley, California. As a side portion of his occupation, he serves as the lab's software troubleshooter. It is during one of these troubleshooting excursions where the books plot takes form.

Stoll is asked to track down a "glitch" in the software which tracks the computer usage on the UNIX based CRAY computer assigned to the lab. In the accounting process, a seventy six- cent unaccountable shortfall is discovered and initially appears to be a low visibility software problem. The thorough validation of the code forces Stoll to discover a much more serious problem which infects a large portion of the ARPANET (early Internet).

As Stoll searches to find the "truth" about the missing time, he discovers misuse of long distance lines, password theft and breaches of networks, both civilian and military. The perpetrator utilizes an operating system rewrite which he places in the host computer much the way a cuckoo bird places her egg in a surrogates nest. The "spy" later returns to retrieve the data collected from the sinister code. This occurs unnoticed by all but the most attentive of system managers across the US.

Stoll goes to great lengths to describe the use of numerous backdoor entrances and trapdoor uses of Unix and computer violation in general. From coding shortfalls to purposely emplaced entrances, Stoll exposes the fairly widespread knowledge and use of

these. He places the blame on computer manufactures, software coders and government watchdogs equally.

As Stoll digs deeper and deeper, he finds the preponderance of material being gathered on military research subjects with keywords "SDI", "stealth", etc. (remember this is '86) Stoll seeks the help of the "three letter agencies" of the US Government and is frustrated and appalled at the lack of interest by the leading agencies. The Central Intelligence Agency (CIA) refuses to investigate due to lack of international evidence. Internally, the Federal Bureau of Investigation (FBI) shows little interest due to the small dollar amount involved. The National Security Agency (NSA) avoids the investigation and cites their charter as passive listeners and not active seekers of information. And, finally the Air Force systems agency attempts to deflect focus due to their fear of security shortfall exposure.

Eventually Stoll tracks down the bad guy with diligence and some timely help from the National Telecommunications Security Committee (of the NSA), International Telegraph and Telephone (ITT), the German Bundespost, and the German police where a line trace is finally done. It is discovered that a hacker in Germany began a "what can I get away with" excursion which developed into a money-making scheme where sensitive documents exchanged hands to Eastern Block nations.

Since the inception of computer attack, network defenders have attempted to keep pace with the increasing complexity and volume of attacks. Computer theft, manipulation and degradation/destruction is spread throughout the cyber world and concerns the corporate world as much as the militaries of the world and the governments that control those militaries.

Historical foundation for use of information warfare.

Several incidents of electronic attack have been chronicled. From the electronic theft of classified documents to the destruction of key information, have they all been observed during the information age. Information theft, money theft, and database disruption are all prevalent actions of the hacker of today.

Dr. Stoll's case study in The Cuckoo's Egg displays not only the eventual resolution on the theft of classified documents but also shows the ability for the cyber thief to steal money in the form of operating system time. In Stoll's account, the discovery of the hacker himself came about because of an operating system accountability shortfall that is discovered at Lawrence Livermore Labs. From a simple mission to find where the missing micro-seconds were Stoll eventually finds an international military theft ring which obtains and sells classified United States documentation.

Computer virus and worms are also widespread in today's digital world. Many viruses are developed to render the operating system of a computer (or network) temporarily useless.²⁰ However, properly developed a worm can make a fully functioning system a digital garbage can. As early as 1988 a worm created by Robert Morris, a Cornell University graduate student, worked its way through the Internet to over 6,000 computers. This worm paralyzed all of these systems which included civilian, military and governmental units. Key to note is the number of systems using the Internet at that time was estimated at 600,000. If a similar worm were developed today with equivalent results, over 2.2²¹ million computers would be affected.

What are some targets?

The options that exist for information warfare and cyber warfare in particular are as varied as the types of systems on the net. A cyber attack waged on a nation could have effects which range from an annoyance for a system administrator to wide spread death. As stated before, to focus only on military targets would be both naive and will leave the path clear for virtually unencumbered entrance into a multitude of targets. To attempt to separate military and civilian systems is also an impossibility given the embedded nature of the NII and DII.

Infrastructure systems within a country are particularly vulnerable and pose a lucrative target for the information warrior. These targets, if successfully manipulated or destroyed, will disrupt the nation to its very core. Telephone switching systems, power grids, financial markets, public transportation systems such as airlines and rail systems, medical and pharmaceutical records as well as the computer networks themselves can all be interfered with if not completely halted.

Additionally, recent attacks have included a modern approach to industrial espionage. The absolute necessity for industry to be constantly connected to the government as well as be available for the public opens those same companies to the risks listed above. Cyber espionage coupled with more traditional rolls of corporate spying carry a crippling potential affect. "Essentially, intrusion has reached its own sort of industrial revolution." ²²

What are the tools used for attack/defense?

The tools for attack are varied and ever changing. Software attack devices range anywhere from the annoying random access memory destroying virus, to software hungry "worms" and instantaneous "logic bombs", to the very complex "sniffer" which reports on account activity and content. For any of these to be effective, access to the information utilized by the target system must be breached. This breach can be by over-the-air media (the Internet) or by air-gap media (diskettes and tape drives). All of these subroutines function on your computer without the attacker's overwatching presence.

The virus is introduced into the computer system from the inclusion of new software and/or the utilization of corrupted data. A virus is actual computer code which is written by the attacker and is attached to a software program or data intended for that software. When a virus is inserted into a bit of data, it automatically attaches itself to the host that is using that data. Then the two virus copies become available for copy in their next use. The computer virus spreads much the same way a bacterial virus would spread in the biological world. Viruses are software type dependent and cannot be transmitted between different types of software. Since the computer is used most widely for correspondence, word processing programs are the battlespace of choice for the virus hacker.

A worm is a more serious form of super-virus. Worms are a series of code which actually destroy resident software on the host computer. Worms are placed in a host computer and then begin to "feed" on the software itself. The code will intertwine itself around the logical programming within the computer until the code fails. This is usually a slow process and takes place over a longer period of time. The user will notice a degradation to the system before total failure. Then the worm dies with the computer.

Most worm programs are directive in nature and do not take on the randomness of the virus.

Another type of software disabler is the logic bomb. The logic bomb is usually constructed with an event in mind. The bombardier will set the bomb to explode on a certain day or at the beginning or end of a certain event such as 1 January 2000, or during the batch run of a financial institutions computer. The bombardier takes advantage of the simplistic basis of the computer and the binary nature of its memory storage. The bomb attacks the logic base of the computer and simply deletes all of the software by changing all of the memory locations to either a logical '1' or '0'. By changing everything to either a '1' or '0' the attacker renders the software unrecognizable and therefore useless.

Our first widespread encounter of this type of attack could be on the first second of the new millennium. The year 2000, or Y2K problem, is the topic of much interest around of the world. Computer systems only read the last two digits of the date. This saves computing time and therefore money. This style of programming assumes that the first two digits of the date are always a "1" followed by a "9". The software reads the date as 19XX. When the new year rings in, the first two digits will be "2" and "0" as in 20XX. The estimated implications of this to the computers and their information vary wildly. Some experts are as apathetic as to say that there will be no impact at all and others stretch to predictions of catastrophic meltdown of all computer networks. The preparation for this and the reaction to network shortfalls will be a major test of computer defense organizations worldwide. In preparation for this single moment in time, the assessment of the vulnerability of systems and the likelihood of a non-time induced attack must be addressed. Similar to the advantage the dawn gives in a small unit attack, the

first second of the first minute of the 1st of January 2000 gives the cyber attacker the same opportunity.

Similar to the logic bomb is a "trap door." A "trap door" is inserted into the controlling code of the host computer and remains dormant until it is activated by the hacker. Routines that are running normally are suddenly affected or destroyed. By utilizing this method, the attacker can gauge when he wishes his deed to be activated.

Perhaps one of the most dangerous forms of attack is the sniffer. The sniffer is placed into a system and reports to the sniffer owner the event of the time period. A sniffer can be set up to report on log-in attempts, web activity, E-mail transmittal, programs accessed, data such as credit card numbers or virtually any activity on that system. It can be broad in nature as it reports on all users sending E-mail or very specific as it reports all time user X accesses program Y. Hackers can watch transfers of electronic money using this technology as well.

The dangerous thing about a sniffer is that unless the system administrator or user detect the placement of the sniffer, they will not know it is there. The one exception to this is the utilization of the web for sniffer transmission of the requested data. The sniffer is basically an illintended computer big brother which tells the requester everything you are willing to tell you host computer.

Attackers can also do their dirty deeds by use of more traditional methods as well. An attacker may use a sniffer to gain password access to a user's account and then actually log on to the system as an impostor. As the user then gains access he has the ability to conduct business as the authorized user would. The transfer of money, sensitive, and damaging information can all be a result of this type of attack.

A final form of attack originates from an origin external to the users system. The processing time of a system can be totally consumed as an E-mail attack is launched. Similar to the harassing phone calls of telemarketers, the attacker can send millions of E-mail messages to a single system. The processing of these messages will cripple the system as the processor or processors of the system attempt to deliver these messages to their intended location. This would be analogous to sending several million letters to a single mailbox in an effort to disrupt the postal service. The difference is the sender does not have to pay thirty-two cents for each message and the recipient can do other functions while the mailman is filling the mailbox.

A coordinated relative to this type of attack is the information blockade. This occurs when the peripheral systems which are connected to the target system are prevented from corresponding with the system itself. The target system is denied access by any of several means including severing of transmission media, bombardment of peripheral systems, agreement, or physical deterrence and cooperation. This type of attack allows the host computer to continue to operate, but does not allow information in or out of the system creating a "dumb"²³ system.

Defense against these attacks and those like them requires diligence, observation, maintenance and virtually continual upgrades to software and other protective measures. Like the pieces of a chess game, the hacker and network manager are in a battle of control of the cyberspace pertaining to the legitimate organization. Making this chess game more complex is the ability for the two players to develop pieces with varied movement schemes and privileges. Within the realm of cyberspace a dance of move/counter move takes place with one or both parties attempting to stay, at least temporarily, anonymous.

What are some defense measures?-

The firewall is the most common tool for attempting network defense. A firewall is software which "acts as a gatekeeper between the Internet and an intranet." This software rejects unwanted packets, and messages therefore, from entering the organizations system. A firewall can also be set up to contain packets within a system to keep certain destination packets from leaving.

The firewall can act in one of two ways. The first queries packets to determine the origination and destination addresses of each packet. Through this it can either accept or reject codes with (or without) certain destination or origination addresses. The second type of firewall is called an application firewall. This firewall actually examines the content of the messages themselves to determine suitability for acceptance. This type of firewall is more cumbersome to the operating system but provides greater protection to the system and its users.

A second type of security measure is the use of cryptographic key and authentication certificates. The current trend in the use of crypto allows the use of public and private keys. The originator of the message sends a public key to the intended user(s). The message is encrypted and then sent to the recipient. If the keys match, the private key used to encrypt the message is successfully decoded by that user's public key, then a successful transmission has occurred. The technological use of this is further rationalized as the originator of the key must obtain a digital certificate which allows the legal use of the unique key and links the user to that key. Through this system, the

messages are passed in a secure manner with the ability to identify positively the originator of the message.

The cutting edge of security was introduced with the JAVA Script programming language. JAVA is an offshoot of C++ and allows Object Oriented Programming (OOP) input and coordination to be relatively safe from intrusion. The JAVA language was developed with the Java Sandbox which allows these applets to be compiled and tested before actually entering the computers memory. This isolates the computer from the input until the code is tested. JAVA sandbox is analogous to quarantine for biological entities.

The most effective defense mechanisms are still the ones which concern themselves with the human interaction with the computer systems. The effective network manager is diligent in his or her network overwatch. System anomalies are thoroughly investigated until the exact root cause for a failure, slowdown, lost password or unauthorized access is discovered. User adherence to policy, or safe computing, remains the key in computer network defense. The periodic changing of passwords, the non-standard password, and strict compliance with network integrity are key weapon systems in the fight for network safety and security.

What are the trends in attack?

The frequency and actions involved in attacks that were reported and/or investigated are but a mere drop in the overall actions being conducted. In 1995 a total of 2400 cyber incidents were reported to the only operating CERT in existence. This team is currently established at Carnegie-Melon and functions as a Special Weapons and

Tactics (SWAT) team for the cyber frontier.²⁴ Compared to the millions of Internet users, and potential attackers, the coefficient of forces is staggeringly low. Although a relatively small organization, the CERT does function as a viable defense force and serves a more valuable function as a guidepost for past, current and emerging trends.

The current efforts being undertaken by attackers are in stark difference to the straightforward intrusions of the 1980s and early 1990s. Although these simple password thefts/bypass schemes and backdoor accesses still exist, the methods have adapted to meet the defense schemes of the good guys. "Intruders are demonstrating increased understanding of network topology, operations and protocols, resulting in the infrastructure attacks described in the previous section on Internet infrastructure."²⁵

Current trends include improved access and exploitation of source code which is readily available and freely obtained. This code is developed often with little eye for security and then is obtained for use by organizations because of its utility and low (or no) cost. This same code is obtained and analyzed by the attacker who discovers and later exploits weaknesses.

Updated Trojan Horse programs enable attackers to be stealthy virtually in their entry and exit into and out of systems. This tried and true technique is supplemented by sophisticated cryptology programs which make the identity, information gathered and path used by and of the attacker virtually indecipherable.

Perhaps the newest and most effective tool of the computer attacker are those which monitor and report on new network connections. These tools allow the attacker to identify quickly infant systems which are void of security or have not fully emplaced

their safeguards. After finding the entry point, attackers can employ any number of techniques for immediate use or can log them for future exploitation.

These tools for attack and defense exist in the unconstrained arena of the cyber world. The creation of these tools on relatively obscure terminals happens with little or no repercussions. The implementation of these tools is when the damage occurs. The users of these tools are governed by laws in their everyday life. What are the laws governing the national and international use of these cyber weapons?

CHAPTER 4

Legalities -

When addressing the legality, or illegality, of cyber use or attack the exact nature of these attacks is neither clear nor defined. In the book Information Warfare and International Law, the authors, Lawrence Greenberg, Seymour Goodman and Kevin Soo Hoo, sum it up when they state, "There is no authoritative legal or international agreement as to whether an IW 'attack' equals an 'attack' or 'use of force' in the traditional sense."²⁶ The lack of legal precedent that allows the United States to pursue IW in order to ensure information dominance is also the opening that an organization will use to exploit the country's vulnerabilities. "The ambiguous state of international law regarding information warfare may leave space for the United States to pursue information warfare activities. Conversely, it may permit adversaries to attack the United States and its systems."²⁷

Complicating this attempt to delineate clearly the rights and wrongs of cyber use are the standing international guidelines which separate the actions in war from peace. "First, it has not been established that information attacks, particularly when they are not directly lethal or physically destructive, constitute the use of force or armed attack under such provisions as the United Nations Charter."²⁸

What are the International laws concerning cyber use?

International law's definition is "the body of rule governing the relations between sovereign states."²⁹ However, a more acceptable definition is an "authoritative institution and process people establish, maintain, and change to aid in the clarification and

achievement of common interests."³⁰ The overall intent of international law is to attempt to govern the actions of nations when dealing with one another. The make up of international law consist of "conventional" law and "customary" law.³¹

"Conventional law is that made by treaty or other explicit agreements among nations, who are bound to their agreements under the principle of *pacta sunt servanda*, or agreements to be observed."³² These agreements can span the range of creation of a worldwide governing body such as the United Nations to treaties on non-proliferation of nuclear weapons to trade agreements. The common thread is the outlook of a mutual goal to be accomplished.

Customary law is derived from the repeated practice of the international community as well as accepted agreements between two or more parties. Nations may recognize customary laws before they are officially ratified on the world scene.

"Customary law results from the general and consistent practice of states' *opinio juris*, or with the understanding that the practice is required by law."³³

The major problem concerning the invocation and support of international laws is the lack of a single governing or legal body which functions as the mechanism for justice and is recognized by the world as a whole. The United Nations Security Council, International Court of Justice and the World Court all attempt to rule on world conventional law, but their abilities are limited by the self determination rights of the sovereign states they act for and upon.

International laws concerning warfare are created to mitigate war's effects on the non-military participants and bystanders of war. The deterring factor for this suffering revolves around the ability for the world to be able to see the suffering caused by the

belligerent. The ability to see the damage and to understand fully that no military target could have been intended are key. United States military strikes against Libya in Operation Eldorado Canyon underscore the importance of full justification of these principles. It also helps to illuminate the similarities of military overflight with information transition over transmission media.

Eldorado Canyon posed the military forces of the United States against targets located deep in Libya. The justification for the attack is retaliation of Libyan sponsored attacks on Berlin. Air Force aircraft based in England were used to attack portions of Libya as well as navy aircraft off of the aircraft carrier USS Enterprise. The damage done to the command and control portions of the Libyan government and military were justified as legitimate. However, the inadvertent strike against the French Embassy was either condemned or seen as collateral damage depending on the point of view of the observer. To further add intrigue to this mission the overflight of French sovereign airspace by United States aircraft was denied adding several hours of flying and a complexity to the mission.

Clouding the issue with information warfare are many of the above-mentioned areas. The overflight issue is much more difficult with respect to information in general because the sender may or may not know the path his information is taking. Observation of these paths is virtually impossible and extremely time consuming and costly at best. Additionally, the intermeshing of civilian and military infrastructure aspects of information management and utilization make the targeting process and damage assessment arena very opaque.

The major problem with the association of information warfare and the international laws is the categorization of information attacks and their relative damage versus a kinetic attack. "[T]he sort of intangible damage that such attacks may cause may be analytically different from the physical damage caused by traditional warfare."³⁴ Within the realm of physical attack, the carnage and destruction visible to the observer clearly denotes "attack." Within the cyber world where attacks are invisible to the casual observer and results may affect processes and not activity, the denotation of attack to an incident may be harder to sell.

What are the United States laws concerning cyber use?

The United States Congress has placed a great deal of emphasis on the legal aspects of the Internet. The majority of the laws passed by the United States have centered around net pornography and network retail and marketing. Support for these laws are strictly handled by municipal, state and federal law enforcement organizations and make up the majority of the efforts expended by these agencies.

Posse Comitatus remains appropriate for the use of US military forces for computer crimes as well. At present, the only involvement the DOD has within the confines of the United States is when it is deemed by the NIPC that national security is at risk, or that a foreign entity is perpetuating the connection. Even when it is deemed a foreign entity is involved, the prospects of national sovereignty and/or defense are considered key for a military response.

Standing DOD Rules of Engagement (ROE) apply for the JTF CND as they do for any military unit. Specifically mentioned in the ROE statements within the CONOPS is

the necessity for the Commander of the JTF to seek SECDEF approval for the initiation of offensive commutur operations. Although this is normally stated on the ROE of many Tasks Force OPORDs, it underscores the immediacy and the current threat for the JTF CND.

What are some historical precedents of convictions (International and US)?

Reports of arrests and convictions of cyber attackers or criminals are both infrequent and underreported. The exhaustive efforts and relative lengthy amounts of time to investigate and prosecute these crimes surpasses the sensationalism of the detection itself. Key cases reported all cite exhaustive efforts by United States Federal officials as well as acknowledging the absolute necessity for international cooperation between governments and civilian organizations as well.

Within the United States, the more sensational cases involved the use of the Internet as a weapon and as a transport device for an electronic device as well. In February of 1995, Kevin Mitnick was arrested for computer theft and corporate damage.³⁵ Mitnick planted several sniffers as well as logic bombs throughout corporations in California, Colorado and North Carolina. All of these intrusions originated from Mitnicks house in Raleigh-Durham, North Carolina thus explaining the interstate portion of the investigation. The Federal Bureau of Investigation (FBI) led the effort and was supported by US Attorneys in Greensboro, North Carolina, San Diego, California and Denver, Colorado.

Seven months later, the United States Secret Service (USSS) arrested seven cyber hackers in an operation dubbed "Operation Cybersnare."³⁶ This case underscores the

interrelated state of the infrastructure. These individuals were caught on a USSS developed bulletin board called Celco 51. The undercover agents advertised this bulletin board as “catering to individuals involved in unauthorized computer intrusion and all aspects of computer fraud, including cellular telephone fraud.”³⁷

The convicted hackers obtained information on the development and procurement of devices involved in the trafficking of stolen and/or cloned cellular telephones. The Internet is used to gain insight, information and equipment to produce the cloned phones. Then, the appropriate electronic information needed to make these illegal clones work is stolen from the cellular company. After completion of the product, the BBS (as well as others) is used to sell the phones at a significantly reduced price. The theft victims range from the local telephone company and the long distance carrier through to the lawful owner of the cellular phone itself.

Similar to the Morris edict stated in the chapters above is the case of Dominick LaScala of Monmouth University. In this case the cyber terrorist acted out of anger with no apparent motivation other than revenge. In November of 1995 LaScala’s computer privileges were suspended by the university because of misuse. Several days later, LaScala utilized two separate E-mail accounts to launch more than 24,000 unsolicited E-mail messages with the same addresses. Two college officials were the intended recipients of these messages. The overabundance of information on the college computer system caused the university’s E-mail system to crash. Repair of the inoperative system cost over \$4000 and Monmouth College reported that over 44 hours needed for the repair. The loss of the \$4000 repair was estimated as one tenth of the loss of the productivity of the lost computer time.

The LaScala case demonstrates the monetary results incurred from down time as well as from repair costs. Key to note is that the \$40,000 estimated in lost computer time is made from an academic source. The loss of 44 hours of corporate computer time could be as much as \$8.6 trillion of this time was lost on the proper system within the international arena.³⁸ Couple these hard dollar figures with the emotional motive and we see the tip of the iceberg with respect to the possible damage by a cyber terrorist.

Within the international arena, cyber warfare mirrors the cases above but takes on a new complexity when attempting to identify and apprehend suspects or attackers. The same international agreements which govern the investigation and extradition of crimes and criminals can cause roadblocks to successful resolution in cyber crime fighting. Most of the cases reported display either absolute coordination between the multiple nations affected or coordination between the hacker and the US. As a case study we can utilize these as examples of individual or small group attacks, but these will be of little or no value in the event of nationally sponsored cyber attacks.

In the summer of 1995, Argentinean Julio Cesar Ardita placed a sniffer within the Departments of Defense and Energy information systems. With this program in place, Ardita received "sensitive information about government research on satellites, radiation and energy."³⁹ Ardita obtained illegal accounts from the computer systems at Harvard University and the Argentine provider Telecom Argentina. Ardita's conquests included sensitive unclassified data from governmental organizations such as the Navy Research Laboratory, NASA's Jet Propulsion Laboratory and Ames Research Center.

Through international cooperation and aided by a court-approved electronic wiretapping device, Ardita was traced and apprehended in Buenos Aires. His computer

system was confiscated by Argentine officials. Ardita agreed to return voluntarily to the United States for trial after a two week interrogation in Argentina. The intended use of the obtained material is still unpublished.

More recent cases of international attack and cooperation include the case of Ehud Tenebaum of Israel. Tenebaum was arrested in March of 1998 by the Israeli National Police for illegally accessing governmental computers of the United States and Israel. This case is key in that it comprised the investigative efforts of one nation and the arrest by another. The United States detected Tenebaum's intrusions into military systems in February of 1998 and formally asked for Israeli assistance in early March. Upon coordinated investigation, it was determined that Tenebaum had accessed Israeli governmental systems as well.

Equally impressive in this case is the elapsed time for the investigation to be completed. With the cooperation of the combined international investigative team as well as corporate efforts, the start to finish time for the investigation was just over two weeks. The cooperation of the team allowed United States Attorney General Janet Reno to state "that the prompt arrest of the Israeli hacker demonstrates the effectiveness of international cooperation in cases involving transnational criminal conduct."⁴⁰

As we review some historical cases of national and international cyber crimes and attacks, we see the increase in both incidents and convictions. The passion of governmental agencies coupled with a new spirit of cooperation among nations gives way to a formidable team in the fight against cyber crime. The same types of actions should fare well in the event a cyber attack is initiated from an individual or smaller organization. It is yet to be seen whether these contingents will be as useful, or even

present, in the event of a nationally sponsored attack. The eventuality of combined cyber warfare at least has a basis from which to begin.

CHAPTER 5

Computer Network Defense Joint Task Force

The Department of Defense established the first Joint Task Force for Computer Network Defense (CND JTF) in 1998. The responsibility for this unit is to identify the source of cyber attacks, assess damage, provide assistance in restarting operations and to provide other expertise. This unit mirrors the national efforts provided by the National Infrastructure Protection Center (NIPC) developed as a result of Presidential Decision Directive 63.

The CND JTF is unique in that it is the first Joint Task Force which is solely controlled by the Secretary of Defense instead of a Unified Commander in Chief (CINC), either regional or specified. This in of itself displays the globalness and overall importance this realm is viewed. The initial commander is an Air Force major general who commands this task force from within the Defense Information Systems Agency (DISA) building in Washington, DC.

What is the mission and how does it support the NSS and NMS?

The mission of this one of a kind and unique unit is "subject to the authority and direction of the SECDEF, CND-JTF will, in conjunction with the Unified Commands, Services and Agencies, be responsible for coordinating and directing the defense of DOD computer systems and computer networks. This mission includes the coordination of DOD defensive actions with non-DOD government agencies and appropriate private organizations."⁴¹

Key portions of the National Security Strategy address information warfare aspects as "we are pursuing a forward-looking national security strategy attuned to the realities of our new era"⁴² As it addresses information warfare, computer attack and hacking it refers to these acts as criminal as well as threats to our "vital interests." The President views this threat across the spectrum and formally unifies the efforts of the country with the National Security Strategy of October 1998. This generalship lays out "a new and systematic approach to fighting the terrorist threat of the next century. It reinforces the mission of the many US agencies roles in defeating terrorism; it also codifies and clarifies their activities in the wide range of US counter-terrorism programs, including apprehension and prosecution of terrorists, increasing transportation security and enhancing incident response capabilities."⁴³

Vital interests are "those of broad, overriding importance to the survival, safety and vitality of our nation."⁴⁴ Important to note within the context of the document is the specific mention of the physical security of our sovereign territory as the number one vital interest. The President clearly links computer intrusion and information warfare to the physical security of our nation when he describes the threats to the United States. "Some foreign intelligence services are rapidly adopting new technologies and innovative methods to obtain such secrets, including attempts to use the global information infrastructure to gain access to sensitive information via penetration of computer systems and networks"^{45 46}

Specific functions of the CND JTF are directly relevant to the NSS as well as Presidential Decision Directives 62 and 63. Functions of the CND JTF are:

- Determine when system(s) are under attack, assess impact to military operations and capabilities, and notify NCA and user community.

- Coordinate/direct appropriate DOD actions to stop attack, contain damage, restore functionality, and provide feedback to user community.

- Develop contingency plans, tactics, techniques, and procedures to defend DOD computer networks; support CINC deliberate planning for same.

- Assess effectiveness of defensive actions and maintain current assessment of operational impact on DOD

- Coordinate as required with NSC, NIPC, law enforcement agencies, other Interagency partners, private sector, and allies.

- Monitor status of DOD computer networks.

- Monitor Intelligence Community and I & W reporting.

- Participate in joint training exercises to conduct CND

- Coordinate with Defense - wide Information Assurance Program (DIAP) and Critical Asset Assurance Program (CAAP) authorities to ensure compliance with wider IA policy and initiatives.

- Provide Intelligence Community with PIR for collection and I & W requirements for potential attacks against DOD computers and networks.

- Subject to authority, direction, and control of SECDEF, provide information to and receive direction from the CJCS, and provide liaison as required to the OSD staff and Joint Chiefs of Staff.⁴⁷

As we see in the multitude of tasks to be performed by the CND JTF, the mission and tasks are both offensive and defensive in nature with the first task as recognition of systems attack.

What is the projected unit environment for the CND JTF?

Unlike any other Joint Task Force ever created within the United States, the CND JTF takes direction from the SECDEF and not from one of the CINCs. This places the CND JTF a direct equivalent to the NIPC and allows commensurate oversight for the entire DOD as well as direct support to all CINCs. The CND JTF provides oversight and direction for all DOD assets with respect to computer intrusion, defense, containment and recovery.

The initial structure of the CND JTF allows for a smooth transition to one of the supporting CINCs. The structure being emplaced mirrors the United States Space Command (USSPACECOM) Regional Satellite Support Center (RSSC) structure. This structure is geographically oriented with centers serving as one stop shopping centers for the DOD space needs. The service provided by the CND JTF will be much the same with a single focal point for computer defense.

The functionality and globalness of the mission of the CND JTF lends itself to this specialized service provision. The forward deployed nature of the proposed structure provides the initial contacts as well as the habitual support which has proven to be so successful.

The CND-JTF acts in concert with other governmental and industrial agencies. Through a combined effort, a formidable defense force can be employed throughout the

front-line of the cyber battlefield of the United States. Given the structure of the units and organizations listed above, what are some of the current efforts being employed to repel or mitigate cyber attacks?

CHAPTER 6

Current defensive efforts and trends -

The United States leads the world in the effort to stem cyber warfare and cyber terrorism. From the October 1998 National Security Strategy through PDDs 62 and 63 the Commander in Chief has made it very clear to the world his views on these issues. The NIPC, in concert with the various CERT teams, poses viable opposition to future adversarial warriors. The ability to detect intrusion coupled with the ability, both technically and legally, to respond to these threats offer the tools for a solid foundation for cyber national defense.

The current trend of information theft will no doubt continue. Information destruction will increase in occurrence as the ability to do so becomes more widespread and less costly. The one constant involved in the field of cyber attack is the ever-occurring update of methods and technology. Similar to the update of military hardware such as tanks and planes, the updates of computer intrusion hardware and software continue to open new avenues of approach into the information manipulation field. Unlike the slow upgrade of a nations military weapons however, computer software is easily distributed with a virtual endless amount of resupply routes with near instantaneous results.

There is a current and real possibility that a nation of small traditional military power can (and will) rise in international stature with the proper utilization of coordinated cyber warfare. Taking advantage of the ambiguity in international law in concert with upgraded computer software, hardware and connectivity, a small nation can wage war

while hiding behind forest of electronic trees. Contending that a nation's infrastructure is of vital importance to the nation and its people, cyber war should be considered warfare using weapons of mass destruction.

Defensive measures being taken-

For the United States to combat effectively computer attacks, an innovative structure must be emplaced which ensures security simultaneous with comfort and unencumbered network functionality. Within the structure of PDDs 62 and 63, a hierarchical scheme of national infrastructure cyber defense is enacted. The Department of Defense portion of this defense in-depth mirrors the CERT teams mentioned above with DOD-specific functions as well.

The lead element for the DOD is the Computer Network Defense Joint Task Force (CND JTF) which is established 8 December 1998. Within the Concept of Operations (CONOPS) the mission of this US military-wide support team is to "be responsible for coordinating and directing the defense of DOD computer systems and computer networks." Through close cooperation with the Defense Information Systems Agency (DISA) as well as the National Security Agency (NSA) the JTF CND provides overwatch, detection, notification and recommendations to the DOD Commanders in Chief (CINCs) and the National Military Command Center (NMCC).

Each of the separate components of the DOD are responsible for the service unique defense of their respective information systems. The Army has proposed a CERT approach which will be directly in line with the NIPC and DOD CERT. This approach allows the best opportunity for seamless flow of information both to and from the DOD

CERT. The ACERT will be located within the general vicinity of the DISA building which promotes joint operations but provides “external lines of communications” from its supported Army elements.⁴⁸

For regional support to Army elements, the ACERT will establish Regional Computer Emergency Response Teams (RCERTs). These support cells will be geographically located in areas where support to Army forces can be most readily achieved.⁴⁹ This concept has proven to be successful for Army (as well as Joint) wide global satellite support and will facilitate any movements to place this element under CINCSpace in the future.⁵⁰

Support for the ACERT is received from both the Army Network & Systems Operations Command (ANSOC) and the Land Information Warfare Agency (LIWA). The ANSOC, located at Fort Huachuca, Arizona under the Army Signal Command (ASC), provides direct support for all ACERT operations. This support includes communications connectivity as well as immediate network support for incidents or events including investigation. LIWA provides general support to include on-call response to events and/or assessment of threat indications and warnings.

Independent of the command and control structure provided by the nation, DOD, or separate services, the main line of defense still remains the individual network managers. Through diligent management of their respective piece of electronic terrain, intrusions and attacks can be detected and dealt with efficiently and effectively. Attentive control of networks ensures that secure/nonsecure exclusiveness is maintained. It also minimizes the ability for backdoor attacks to succeed due to prolonged negligence of network usage.

Commanders share the burden of information security when monitoring the information placed on their respective web locations. The amount of open source information available concerned the DOD and prompted the August 1998 Internet Inclusion Policy which limited information placed on unit web pages. This was a key step in the projection of concern for information leakage for the DOD.

CHAPTER 7

Conclusion-

The computer offers the belligerent of today an ability to attack infant nations, as well as super powers on a level of offensive parity. The effects of a properly executed and successful cyber attack can effect results on a nation's infrastructure which can cause damage rivaling those caused by weapons of mass destruction. Network defense for these infrastructure information systems and those like them is a real and necessary function of a sovereign nation. The warfare waged in this realm extends beyond the traditional military arena to encompass the nation's service industry, industrial base and into virtually every aspect of the society itself.

Through the combined efforts of other aggressors and the theft of well intended computer tools, the attacker of today has an endless supply of cyber weapons. The weapons used for cyber attack keep increasing in both number, complexity and lethality. Trends in attack show an ever increasing occurrence with a frightening ability for the attacker to cloak his activities. Defense mechanisms against these systems are hard pressed to keep pace with the staggering numbers of attacks and the technological aspects of them as well. Combine these with other mitigating factors which constrain the good guys and the task of computer network defense is a formidable.

Laws governing the utilization of the interconnected web known as the Internet cannot govern the legitimate use of this entity, much less the adversarial use of it. The international agreements in place to attempt to mitigate negative aspects of usage provide little coverage when the entry points into the system are endless.

The detection of a computer attack is difficult enough but possible with a vigilant, coordinated and aggressive defense structure. The United States poses a viable defense option for the information systems of this country through its structure which includes CERT and CND-JTF type assets. Through organizations such as these, attackers can be identified in a timely manner and their effects negated or minimized. Attackers now have a viable foe in the battle for electronic cyber battlespace.

ENDNOTES

¹ Clausewitz, *On War*, ed. and translated by Micheal Howard and Peter Paret, (Princeton, NJ: Princeton Universtiy Press, 1989) 526.

² By this I refer to the incorporation of the entire will of the people to the effort. Although Mao's theory concentrated on a three stage revolution, his views of the enemy as a whole (including the civilian populace) are relevant in today's cyberattack strategy.

³ Anne Wells Branscomb, *Who Owns Information?*, From Privacy to Public Access (New York: Basic Books, 1994), 1.

⁴ 35 billion phones are now in existence compared to the number of computers in use.

⁵ Clifford Stoll, *The Cuckoo's Egg*. New York: Doubleday. 1989, 59.

⁶ Power refers to the computing power of the computer system. This is widely accepted as the processing speed of the computer (including collocated and distributed memory) associated with the mental capabilities of the operator.

⁷ Stoll, 302.

⁸ The NII and DII contain and are made up of all communications systems that provide communications support to the nation and the DOD respectively. The Internet and its military counterpart the NIPRNET and SIPRNET also utilize and makeup the DII. Voice, video, imagery and teletype communications systems are also included in the DII with paging, PCS, etc systems making up the NII.

⁹ Defense Information Systems Agency (DISA) briefing DII - Integrating Global Operations ... The Road Ahead, www.disa.mil/D7/briefing/slide7.

¹⁰ John M Shalikashvili, *Information Warfare A Strategy for Peace ... The Decisive Edge in War*, 2.

¹¹ Thomas Rona, early proponent of information warfare and information dominance as quoted in *What is Information Warfare?*, by Martin Libbicki (Washington DC: National Defense University Press, 1995).

¹² William J. Clinton, *A National Security Strategy for a New Century*, October 1998, 18.

¹³ Clausewitz, 75.

¹⁴ Lawrence T Greenburg, Seymour E Goodman, Kevin J Soo Hoo. in *Information Warfare and International Law* (Washington DC: National Defense University Press. 1998) while setting the stage for the complexity of not only executing information warfare, but attempting to codify the legal ramifications of it.

¹⁵ John D. Howard, *An Analysis of Security Incidents On The Internet 1989 - 1995*, Doctoral Dissertation, Carnegie Mellon University, 7 April 1997, Chapter 7, 1.

¹⁶ Ibid, Ch 7, 1.

¹⁷ Ibid, Ch 7, 1.

¹⁸ Data is compiled by Dr., John D. Howard, *An Analysis of Security Incidents On The Internet 1989 - 1995*, Doctoral Dissertation, Carnegie Mellon University, 7 April 1997, Chapter 2, Figure 2.3.

¹⁹ Thomas Lonstaff, *Information Warfare*, The Learning Channel documentary, October 1998.

²⁰ Most viruses found on today's personal computer actually do little damage to the computer or its information. The viruses found, for the most part, simply effect the random access memory (RAM) of the system which effects the current application, but does little to alter or destroy long term stored data.

²¹ Data provided by Mr. Karl Rubin of Technology Builders Incorporated (TBI) of Marietta, Ga. This data deals with the loss of computing time associated with computer outages of any kind. Costs associated ranged from \$20,000/minute on the SABRE reservation system of American Airlines to \$1 million/minute for Schwab Investment including lost sales and trades.

²² Jean Guisnel, *CYBERWARS, Espionage on the Internet*, (New York:Plenum Press. 1997)76.

²³ The term "dumb" was used in early computer days and it describes a terminal that was not networked to other computers within a workplace. These terminals usually performed the same tasks as the "smart" terminals, but information would be hand carried between the terminals vice transmitted over the interconnection media.

²⁴ C. Molander. & Andrew Riddle, *A New Face of War*, The Learning Channel documentary, October 1998.

²⁵ Marcel Dekker, *The Froelich/Kent Encyclopedia of Telecommunications*, vol. 15. The infrastructure attacks mentioned include probes, scans, account compromises, root compromises, sniffers, and service denials.

²⁶ Greenburg, 26.

²⁷ Ibid, xviii.

²⁸ Ibid, xvii.

²⁹ Grolier electronic encyclopedia 1996 version.

³⁰ Ibid.

³¹ Vienna Convention on the Law of Treaties (1969). United Nations Document A/CONF 39/27.

³² Henkin, Louis, *International Law: Politics and Values*, 38-39

³³ Greenburg, 7.

³⁴ Ibid, 9.

³⁵ Kevin Mitnick's actual conviction was in June of 1997. At the time of his arrest, Mitnick was on probation for the same type of cyber criminal activity which occurred in 1992. The total prison sentence for the two convictions is 36 months (14 for the first conviction and 22 for the second). Mitnick also incurred 3 years supervised probation which includes stipulations that Mitnick can have no access, including ownership, to computers without express consent of his probation officer.

³⁶ Department of Justice, Press Release, *Cybersnare Sting Operation News Release*, 11 Sep 1995, 1.

³⁷ Ibid, 2.

³⁸ 24 hours of computer time of a brokerage firm (see note 21).

³⁹ Department of Justice, Press Release, Argentine Computer Hacker Agrees to Waive Extradition and Returns to Plead Guilty to Felony Charges in Boston, 29 March 1996.

⁴⁰ Department of Justice, Press Release, Israeli Citizen Arrested in Israel for Hacking United States and Israeli Government Computers, 18 March 1998.

⁴¹ As per the Computer Network Defense Joint Task Force (CND JTF) Working Group final in progress review (IPR) dtd. 18 September 1998. This IPR only projects the mission statement. Approval of the mission statement is projected for 6 November 1998.

⁴² Clinton, iii

⁴³ Ibid, 5.

⁴⁴ Ibid, 5.

⁴⁵ The secrets discussed are those discussed earlier in the paragraph as American military, diplomatic, technological and commercial secrets.

⁴⁶ Clinton, 7.

⁴⁷ As per the Computer Network Defense Joint Task Force (CND JTF) Working Group final in progress review (IPR) dtd. 18 September 1998. This IPR only projects the mission statement. Approval of the mission statement is projected for 6 November 1998.

⁴⁸ As presented in the Army DCSOPS briefing on JTF-CND COMARFOR Alternatives decision briefing, December 1998. The external lines of communications refers to the physical and electronic location of the ARFOR element which will be collocated with the Joint element versus under the Pentagon Army element. The command structure still remains clearly under the Chief of Staff of the Army.

⁴⁹ This RCERT architecture mirrors the support concept established in the US Space Command (USSPACECOM) with its Regional Satellite Support Centers (RSSCs). The RSSCs are currently located in Germany, Japan, Hawaii and Washington, DC.

⁵⁰ The future positioning and Command and Control of the JTF-CND as well as any of its subordinate organizations is currently planned to be placed under the command of CINC SPACE. The mirroring of the SPACECOM command structure would provide for a comfortable seamless transfer to fully operational capabilities (FOC) status when that decision is made.

SELECTED BIBLIOGRAPHY

Books

Alberts, David S. *Defensive Information Warfare*. Washington DC: National Defense University Press. 1996.

_____; *The Unintended Consequences of Information Age Technologies*. Washington DC: National Defense University Press. 1996.

_____; Papp, Daniel S. *Information Age Anthology (Parts 1-4)*. Washington DC: National Defense University Press. 1997.

Allard, Kenneth C. *Command, Control and the Common Defense*. New Haven: Yale University Press, 1990.

Arquilla, John and David Ronfeldt, with foreword by Alvin and Heidi Toffler, *In Athena's Camp*. Santa Monica, CA: RAND 1997.

Campen, Alan D., Douglas D. Heath and R Thomas Gooden. *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax, VA: AFCEA International Press, 1996.

Clausewitz, Carl von. *On War*, ed. and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1989.

Creveld, Martin van. *The Transformation of War*. New York, NY: The Free Press, 1991.

Fuller, John Frederick Charles. *The Foundations of the Science of War*. London: Hutchinson & Co. LTD., 1926; a military classic reprint, Fort Leavenworth, KS: US Army Command and General Staff College Press, 1993.

Greenberg, Lawrence; Goodman, Seymour; Soo Hoo, Kevin. *Information Warfare and International Law*. Washington DC: National Defense University Press. 1998.

Guisnel, Jean. *Cyberwars: Espionage on the Internet*. New York: Plenum Press. 1997.

Johnson, Douglas V. *AY 97 Compendium, Army After Next Project*. Pennsylvania: Strategic Studies Institute. 1998.

Johnson, Stuart E.; Libicki, Martin C. *Dominant Battlespace Knowledge*. Washington DC: National Defense University Press. 1996

Libicki, Martin C. *The Mesh and the Net*. (2nd Printing). Washington DC: National Defense University Press. 1995.

_____; *Defending Cyberspace and Other Metaphors*. Washington DC: National Defense University Press. 1997.

_____; *What is Information Warfare?*. Washington DC: National Defense University Press. 1995.

Nichiporuk, Brian and Carl H. Builder. *Information Technologies and the Future of land Warfare*. Santa Monica, CA: RAND, 1995.

Schwartau, Winn. *Information Warfare, Chaos on the Electronic Superhighway*. New York, NY: Thunder's Mouth Press, 1994.

Smith, Merritt Roe and Leo Marx, *Does Technology Drive History? The Dilemma of Technological Determinism*, Cambridge, MA: The MIT Press, 1994.

Stoll, Clifford. *The Cuckoo's Egg*. New York: Doubleday. 1989.

Toffler, Alvin and Heidi. *War and Anti War*. New York: First Warner Books Printing, 1995.

Waldrop, W Mitchell, *Complexity, The Emerging Science at the Edge of Order and Chaos*. New York, NY: Touchstone Book, 1992.

Articles

Boorda, Jeremy M., "Leading the Revolution in C4I," Joint Force Quarterly (Autumn 1995).

Brewin, Bob. "Cyberattacks leave feds chasing 'vapor'," Federal Computer Week (June 15, 1998): p. 3-5.

Bridis, Ted. "Complex computer code fails," The Kansas City Star (July 18, 1998): A-5.

Burton, Daniel F., "The Brave New Wired World," Foreign Policy (Spring 1997) pp. 23-38.

Campbell, Matt. "Hackers hit military's computers," The Kansas City Star (February 26, 1998): A-2.

Cheswick, William and Steven M Bellovin, "How Computer Security Works, Firewalls," Scientific American, (October 1998): 106-107.

Cole, Richard. "FBI searches homes in Pentagon hacking case," The Leavenworth Times (February 27, 1998): A-12.

Dearth, Douglas H. "Information War: Rethinking the Application of Power in the 21st Century," Military Intelligence Professional Bulletin, Volume 23 Number 1 (March 1997): 11-16.

Ford, Warwick. "How Computer Security Works, Digital Certificates," Scientific American, (October 1998): 108.

Gumahad, Arsenio T., "The Profession of Arms in the Information Age," Joint Force Quarterly, (Spring 1997), p19.

McConville, James E. "US Army Information Operations: Concept and Execution," Military Intelligence Professional Bulletin, Volume 23 Number 1 (March 1997): 17-22.

Meinel, Carloyn P. "How Hackers Break In ... and How They Are Caught," Scientific American, (October 1998): 98-108.

Reardon, Thomas M. "Information Warfare: Protecting Force Sustainment," Military Intelligence Professional Bulletin, Volume 23 Number 1 (March 1997): 25-27.

Rivest, Ronald L. "The Case against Regulating Encryption Technology," Scientific American, (October 1998):

Seffers, George I. "Pentagon Resurrects Top C3I Office," Defense News (February 16 - 22, 1998): 1, 18-19.

Monographs and Theses

Boslego, David V. The Relationship of Information to the relative combat power in Force XXI Engagements. MMAS monograph, School of Advanced Military Studies, United States Army Command and General Staff College, FT Leavenworth, 1995.

Hengst, Paul T.. managing the Intelligent Information Grid for the Army After Next, Army After Next Project AY 97 Compendium, U.S. Army War College, 1997.

Howard, John D. An Analysis of Security Incidents on the Internet 1989-1995, Doctoral Dissertation, Carnegie-Mellon University, Pittsburgh, PA, 7 April 1997.

Hurst, Elizabeth A. Shaping the Battlefield with Command and Control Warfare. MMAS monograph, United States Army Command and General Staff College, FT Leavenworth, 1996.

Landecker, David. The Virtual Army: Management Concepts for an Information Age Army. MMAS monograph, United States Army Command and General Staff College, FT Leavenworth, 1996.

Rodgers, James L. Information Warfare: Lessons from World War Two. Monograph, Marine Corps War College, Marine Corps University, Quantico, 1996.

Smith, Kevin B. The Crisis and Opportunity of Information War. MMAS monograph, School of Advanced Military Studies, United States Army Command and General Staff College, FT Leavenworth, 1994.

Swan, Robin P. The Pieces of a Military Chessboard-What is the Contemporary Significance of Jomini's Design of a Theater of Operations? MMAS monograph, School of Advanced Military Studies, United States Army Command and General Staff College, FT Leavenworth, 1991.

Uchida, Ted T. Building a basis for information warfare rules of engagement. MMAS monograph, School of Advanced Military Studies, United States Army Command and General Staff College, FT Leavenworth, 1997.

Woods, Kevin S. The Changing Application of Maneuver. MMAS monograph, School of Advanced Military Studies, United States Army Command and General Staff College, FT Leavenworth, 1996.

Government Documents

"Combating Terrorism: Presidential Decision Directive 62": Washington, DC: (accessed 4 December 1998) available from <http://www.fas.org/irp/offdocs/pdd-62.htm>

Office of the Joint Chiefs of Staff, *Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare (C2W)*, Washington, DC: 7 February 1996.

President of the United States, *A National Security Strategy For A New Century*. Washington, DC: U.S. Government Printing Office, October 1998.

"Protecting America's Critical Infrastructure: Presidential Decision Directive 63": Washington, DC: (accessed 4 December 1998) available from <http://www.fas.org/irp/offdocs/pdd-63.htm>

Shalikashvili, John M. *Information Warfare A Strategy for Peace... The Decisive Edge in War*. Pamphlet; Washington, DC: U.S. Department of Defense, undated.

US Army. *Field Manual 100-1, The Army*. Washington, DC: U.S. Government Printing Office, October 1994.

_____. *Field Manual 100-5, Operations*. Washington, DC: U.S. Government Printing Office, June 1993.

_____. *Field Manual 101-5-1, Operational Terms and Symbols*. Washington, DC: U.S. Government Printing Office, 1997.

_____. *Revised Final Draft Field Manual 100-5, Operations*. Washington, DC: U.S. Government Printing Office, 19 June 1998.

_____. *Coordinating Draft Field Manual 100-6, Information Operations*. Washington, DC: U.S. Government Printing Office, 1998.

E-Mail and Other Electronic Documents

“Argentine Computer Hacker Agrees to Waive Extradition and Returns to Plead Guilty to Felony Charges in Boston”, United States department of Justice, Press Release, undated, (accessed 11 December 1998), available from <http://www.usdoj.gov/usao/ma/pr/prev98/arditasnt.html>

Bibliography of Information Warfare and Infrastructure Vulnerability Documents, (accessed 18 August 1998), available from http://www.aracnet.com/~gtr/archive/info_war.html.

Carney, Kenneth, Technology Builders Incorporated (TBI), Marietta, GA. response to question concerning cost of computer down time. 2 January 1999.

Command, Control, Communications, Computers and Intelligence (C4I) Institute for Strategic Research Cooperative Research Program (CCRP), (accessed 24 August and 13 September 1998), available from <http://www.dodccrp.org>.

“Computer Hacker Kevin Mitnick Sentenced to Prison”, United States Department of Justice, Press Release, 27 June 1997, (accessed 11 December 1998), available from <http://www.usdoj.gov/usao/cac/pr/cac70627.1.html>.

Computer Network Defense Joint Task Force Working Group Update, Briefing given 18 September 1998, Washington, DC.

"Cybersnare--Arrests", United States Department of Justice, Press Release, 9 November 1995, (accessed 11 December 1998), available from <http://www.usdoj.gov/usao/nj/news/1995press/nj62.txt.html>.

Defense Advanced Research Projects Agency (DARPA), (accessed on 21 December 1998), available from <http://www.darpa.mil>.

Defense Information Systems Agency (DISA), (accessed 22 November 1998), available from <http://www.disa.mil/D7/briefing/start.html>.

"Federal Cybersleuths Armed with First ever Computer Wiretap Order Net International Hacker Charged with Illegally Entering Harvard and U.S. Military Computers", United States Department of Justice, Press Release, 29 March 1996, (accessed 11 December 1998), available from <http://www.usdoj.gov/opa/pr/1996/March96/146.txt>.

"Fugitive Computer Hacker Arrested in North Carolina", United States department of Justice, Press Release, 15 February 1995, (accessed 11 December 1998), available from http://www.usdoj.gov/opa/pr/Pre_96/February95/89.txt.html.

"Growth and Usage of the Web and the Internet", Internet Growth and Statistics, (accessed 10 and 13 December 1998), available from <http://www.mit.edu/people/mkgray/net/printable>.

Institute for the Advanced Study of Information Warfare (IASIW), (accessed 18, 22, 30 August 1998, 5, 7, 30 September 1998), available from <http://psycom.net/iwar.1.html>.

Information Warfare Links, (accessed 1,7,19 November 1998) available from <http://www.tno.nl/instit/fel/intern/wkiwar5.html>.

"Israeli Citizen Arrested in Israel for hacking United States and Israeli Government Computers", United States Department of Justice, Press Release, 18 March 1998, (accessed 11 December 1998), available from <http://www.usdoj.gov/opa/pr/1998/March/125.htm.html>.

"LaScala, Dominick -- Complaint", United States Department of Justice, Press Release, 28 November 1995, (accessed 11 December 1998), available from <http://www.usdoj.gov/usao/nj/news/1995press/nj139.txt.html>.

Lickteig, Fred W., LTC United States Marine Corps, "Information Warfare and Principles of War", unpublished paper, 26 February 1998.

National Information Protection Center (NIPC), (accessed 10 and 13 December 1998, 4,5, 11 January 1999), available from <http://www.fbi.gov/nipc/bome.htm>.

Rubin, Karl S, Technology Builders Incorporated (TBI), Marietta, GA. response to question concerning cost of computer down time. 14 December 1998.

Solimene, Patricia, CPT, United States Space Command, Colorado Springs, CO. response to question concerning Regional Satellite Support Centers. 5 January 1999.

The Internet Index, (accessed 13 Decemebr 1998), available from
<http://www.openmarket.com/intindex.cfm>